

GALOIS REPRESENTATIONS FROM PRE-IMAGE TREES: AN ARBOREAL SURVEY

RAFE JONES

Dedicated to the late R. W. K. Odoni, whose inquisitive spirit led him before any others to these beautiful questions.

ABSTRACT. Given a global field K and a rational function $\phi \in K(x)$, one may take pre-images of 0 under successive iterates of ϕ , and thus obtain an infinite rooted tree T_∞ by assigning edges according to the action of ϕ . The absolute Galois group of K acts on T_∞ by tree automorphisms, giving a subgroup $G_\infty(\phi)$ of the group $\text{Aut}(T_\infty)$ of all tree automorphisms. Beginning in the 1980s with work of Odoni, and developing especially over the past decade, a significant body of work has emerged on the size and structure of this Galois representation. These inquiries arose in part because knowledge of $G_\infty(\phi)$ allows one to prove density results on the set of primes of K that divide at least one element of a given orbit of ϕ .

Following an overview of the history of the subject and two of its fundamental questions, we survey in Section 2 cases where $G_\infty(\phi)$ is known to have finite index in $\text{Aut}(T_\infty)$. While it is tempting to conjecture that such behavior should hold in general, we exhibit in Section 3 four classes of rational functions where it does not, illustrating the difficulties in formulating the proper conjecture. Fortunately, one can achieve the aforementioned density results with comparatively little information about $G_\infty(\phi)$, thanks in part to a surprising application of probability theory, as we discuss in Section 4. Underlying all of this analysis are results on the factorization into irreducibles of the numerators of iterates of ϕ , which we survey briefly in Section 5. We find that for each of these matters, the arithmetic of the forward orbits of the critical points of ϕ proves decisive, just as the topology of these orbits is decisive in complex dynamics.

1. INTRODUCTION

In this survey, we lay out recent work on the action of the absolute Galois group of a global field on trees of iterated pre-images under rational functions. These actions, also known as *arboreal Galois representations*, have recently seen a surge in interest, largely due to their applications to certain density questions. Their study dates to the foundational work of R. W. K. Odoni [35, 36, 37] in the 1980s. Odoni aimed in part to study recurrence sequences satisfying relations of the type $a_n = f(a_{n-1})$, where $a_0 \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree at least two. Such a sequence may be described as the orbit of a_0 under the dynamical system given by iteration of $f(x)$. One might ask whether the sequence $(a_n)_{n \geq 0}$ contains infinitely many primes, but this seems

completely out of reach at present. Indeed, the sequence (a_n) grows extremely quickly – on the order of d^{d^n} – and a heuristic argument suggests that only finitely many of the a_n are prime. To illustrate the difficulty of this problem, note that taking $a_0 = 3$ and $f(x) = (x - 1)^2 + 1$ yields the Fermat numbers, whose prime decompositions have been a mystery since Fermat first speculated about them in 1640. A more reasonable hope is to obtain some qualitative information about the prime factorizations of the a_n , for instance by considering the whole collection

$$P_f(a_0) := \{p \text{ prime} : p \text{ divides at least one non-zero term of } (a_n)_{n \geq 0}\}.$$

If this set is sparse within the set of all primes, then at least the a_n do not in the aggregate have too many small prime factors. Another natural question, which we do not discuss in this survey, is whether all but finitely many terms of the sequence (a_n) have a primitive prime divisor (that is, a prime divisor that does not divide any previous terms of the sequence). For a sampling of the large and interesting literature on this question, which merits a survey of its own, see [10, 12, 18, 26, 42, 45].

It was Odoni who in [35, 36] first recognized that if the Galois groups $G_n(f)$ of the iterates $f^n(x)$ of $f(x)$ satisfy certain properties, then $P_f(a_0)$ has natural density zero in the set of all primes (see p. 20 for a definition of natural density). Indeed, the density of the complement of $P_f(a_0)$ is bounded below by the density of p such that $f^n(x) \equiv 0 \pmod p$ has no solution (see p. 21 for more on this). The latter condition is equivalent to Frobenius at p acting without fixed points on the roots of $f^n(x)$. One then gets from the Chebotarev density theorem (in fact, the Frobenius density theorem suffices [49, Section 3]) that $P_f(a_0)$ has density zero if

$$(1) \quad \lim_{n \rightarrow \infty} \frac{\#\{g \in G_n(f) : g \text{ fixes at least one root of } f^n(x)\}}{\#G_n(f)} = 0.$$

Odoni exploits this observation in [36], where he considers *Sylvester's sequence*¹, defined by

$$w_1 = 2, \quad w_n = 1 + w_1 w_2 \cdots w_{n-1} \quad \text{for } n \geq 2.$$

One readily checks that $w_n = w_{n-1}^2 - w_{n-1} + 1$, and so Sylvester's sequence is the orbit of 2 under iteration of $f(x) = x^2 - x + 1$. Odoni proves the highly non-trivial result that $P_f(2)$ has density zero in the set of all primes by establishing isomorphisms

$$(2) \quad G_n(f) \cong \text{Aut}(T_n) \quad \text{for all } n \geq 1,$$

where $G_n(f)$ is the Galois group of the n th iterate of $f(x) = x^2 - x + 1$ and $\text{Aut}(T_n)$ is the group of tree automorphisms of the complete binary rooted tree of height n . The tree in question has as its vertex set the disjoint union $\{0\} \sqcup f^{-1}(0) \sqcup f^{-2}(0) \sqcup \cdots \sqcup f^{-n}(0)$ of iterated preimages of 0 under $f(x)$, and two vertices are joined by an edge when f sends one vertex to the other. That $G_n(f)$ injects into $\text{Aut}(T_n)$ follows from basic Galois theory; to prove surjectivity requires the art. With the explicit description of

¹Named for J. J. Sylvester, and known widely for its connections to Egyptian fractions.

$G_n(f)$ given in (2), Odoni goes on to establish (1) by a direct calculation [36, p. 5], a result which has a nice restatement in terms of branching processes [21, Proposition 5.5]. It is worth pointing out that isomorphisms such as those in (2) do not hold for $f(x) = (x - 1)^2 + 1$; in this case $G_n(f)$ may be shown to be abelian, and the corresponding zero-density result follows easily [36, p. 11].

Odoni did not use the language of tree automorphisms, preferring to think of $\text{Aut}(T_n)$ as the n -fold iterated wreath product of $\mathbb{Z}/2\mathbb{Z}$ (or more generally of S_d when the tree is d -ary for $d \geq 2$). For us, considering elements of $G_n(f)$ as tree automorphisms has the advantage of providing an object on which Galois acts, thus allowing a more direct analogy with Galois representations associated to abelian varieties. We note that another dynamical Galois representation comes from the natural Galois action on the set of periodic points of ϕ . We do not treat this interesting topic in the present article, but see [29], [30], and [47, Section 3.9].

1.1. Definitions and main questions. To more closely match the Tate module from the theory of abelian varieties, we wish to attach an infinite pre-image tree to any rational function $\phi \in K(x)$ of degree $d \geq 2$ and any point $\alpha \in \mathbb{P}^1(K)$, where K denotes a global field with separable closure K^{sep} . Denote by $\phi^n(x)$ the n th iterate of ϕ , that is, the n -fold composition of ϕ with itself. We must be careful to consider *only* α for which the equation $\phi^n(x) = \alpha$ has d^n distinct solutions, for each $n \geq 1$. This ensures that we obtain a complete infinite rooted d -ary tree $T_\infty(\alpha)$ whose set of vertices is

$$(3) \quad \bigsqcup_{n \geq 0} \phi^{-n}(\alpha) \subseteq \mathbb{P}^1(K^{\text{sep}})$$

and whose edges are given by the action of ϕ (we take $\phi^0(\alpha) = \{\alpha\}$ in (3), and note that α is the root of the tree). The absolute Galois group $\text{Gal}(K^{\text{sep}}/K)$ acts on $T_\infty(\alpha)$, and moreover preserves the connectivity relation in $T_\infty(\alpha)$, as Galois elements commute with ϕ since the latter is defined over K . Hence we obtain a homomorphism

$$\rho : \text{Gal}(K^{\text{sep}}/K) \rightarrow \text{Aut}(T_\infty(\alpha)).$$

The image of ρ is the primary object of study in this article, and we write

$$G_\infty(\phi, \alpha) := \text{im } \rho.$$

More concretely, $G_\infty(\phi, \alpha)$ is the inverse limit of the Galois groups

$$G_n(\phi, \alpha) := \text{Gal}(K(\phi^{-n}(\alpha))/K),$$

which form an inverse system under the natural surjections $G_{n+1}(\phi, \alpha) \rightarrow G_n(\phi, \alpha)$ that arise from the inclusions $K(\phi^{-n}(\alpha)) \subseteq K(\phi^{-(n+1)}(\alpha))$. If h is a Möbius transformation defined over K and $\psi := h^{-1} \circ \phi \circ h$, then a simple calculation shows that $K(\phi^{-n}(\alpha)) = K(\psi^{-n}(h^{-1}(\alpha)))$ for each $n \geq 1$. Taking h to be translation by α , we see that to determine $G_\infty(\phi, \alpha)$, we need only determine $G_\infty(\psi, 0)$, and hence to obtain complete

knowledge in the general situation it is enough to understand the case where $\alpha = 0$. In the sequel, we thus drop any reference to α and write

$$\boxed{T_\infty \text{ for } T_\infty(0), \quad G_\infty(\phi) \text{ for } G_\infty(\phi, 0), \quad G_n(\phi) \text{ for } G_n(\phi, 0).}$$

In light of the definition of ρ , we have natural injections

$$G_\infty(\phi) \hookrightarrow \text{Aut}(T_\infty) \quad \text{and} \quad G_n(\phi) \hookrightarrow \text{Aut}(T_n),$$

where the vertex set of T_n is $\bigsqcup_{i=0}^n \phi^{-i}(0)$, and edges are assigned according to the action of ϕ . We emphasize that throughout this article,

we assume that for each $n \geq 1$, $\phi^n(x) = 0$ has d^n distinct solutions in K^{sep} .

This assumption is a mild one, and can be easily checked for a given ϕ . With these conventions in place, we pose our first main question:

Question 1.1. Let K be a global field.

- (a) For which rational functions $\phi \in K(x)$ do we have $[\text{Aut}(T_\infty) : G_\infty(\phi)] < \infty$?
- (b) For which ϕ do we have $G_\infty(\phi) = \text{Aut}(T_\infty)$?

We remark that the finite index question is perhaps more robust, since a positive answer implies a positive answer when K is replaced by any finite extension. In the well-studied case of ℓ -adic Galois representations arising from elliptic curves, J.-P. Serre settled the analogue to Question 1.1(a) with his celebrated open image theorem [44]. Let E be an elliptic curve without complex multiplication and defined over a number field K , ℓ a rational prime, and G_∞ the inverse limit of the Galois groups of the extensions $K(E[\ell^n])/K$. Because of the group structure on E , one has a natural injection $G_\infty \hookrightarrow \text{GL}(2, \mathbb{Z}_\ell)$. Serre showed that

$$(4) \quad [\text{GL}(2, \mathbb{Z}_\ell) : G_\infty] < \infty,$$

with the index being 1 for all but finitely many ℓ . The proof of Serre's theorem relies on the relative paucity of subgroups of $\text{GL}(2, \mathbb{Z}_\ell)$. In our dynamical setting, on the other hand, one finds that $\text{Aut}(T_\infty)$ has a discouraging abundance of subgroups; for instance when $d = 2$, every countably based pro-2 group is a subgroup of $\text{Aut}(T_\infty)$, and matters are at least as bad for larger d . Nonetheless, some techniques are available for showing that $G_\infty(\phi)$ must be a large subgroup of $\text{Aut}(T_\infty)$ in certain cases, and we survey them and the results they provide in Section 2. In addition, we provide some evidence supporting the idea that Question 1.1(a) has an affirmative answer in general.

Question 1.1(a) does not have a positive answer for all ϕ , just as Serre's theorem does not hold when E has complex multiplication, but in attempting to make a precise conjecture one encounters serious obstacles in locating the cases that must be excluded. In Section 3, we discuss in some detail four types of these exceptional maps, including those that are post-critically finite (see p. 7 for a definition) and those that commute with a non-trivial Möbius transformation. In the case where ϕ is quadratic, enough

results and examples have now been accumulated that we conjecture these four types constitute the only exceptions (see Conjecture 3.11).

To prove zero-density theorems for primes dividing a given orbit of ϕ , one does not need information as strong as $[\text{Aut}(T_\infty) : G_\infty(\phi)] < \infty$. This raises our second primary question:

Question 1.2. Let K be a global field. For which maps $\phi \in K(x)$ can we deduce enough about $G_\infty(\phi)$ to ensure that the limiting proportion of fixed points given in (1) is zero, and hence all orbits of ϕ have density zero prime divisors?

In Section 4, we survey results showing that in some cases minimal information about $G_\infty(\phi)$ suffices. These results proceed via a possibly unexpected use of the theory of stochastic processes, and they lead to a variety of zero-density theorems (see Theorem 4.3 for an example). Many of the results in Sections 2 and 4 rely on being able to establish that the numerators of ϕ^n are irreducible for all $n \geq 1$. Results in this direction, which are of interest in their own right, are surveyed in Section 5.

2. THE IMAGE OF ρ : GENERIC CASE

2.1. A tour of known results. Let $\rho, G_\infty(\phi)$, and $G_n(\phi)$ be defined as on p. 3. Any discussion of the generic situation must begin with work of Odoni, who in [35] studied the case where K is a field of characteristic zero, t_0, \dots, t_{d-1} are algebraically independent over K , and

$$(5) \quad F(x) = x^d + t_{d-1}x^{d-1} + \dots + t_1x + t_0.$$

Let T_∞ be defined as in (3) with $\phi = F$; now it resides in the algebraic closure of $K(t_0, \dots, t_{d-1})$. Odoni shows [35, Theorem I]:

Theorem 2.1 ([35]). *With notation as above, $G_\infty(F) = \text{Aut}(T_\infty)$.*

In the case where K is a number field, one may then fix n and apply Hilbert's irreducibility theorem to deduce that $G_n(f) = \text{Aut}(T_n)$ for all but a "thin set" E_n of degree- d polynomials f defined over K . Unfortunately, E_n is not effectively computable, and moreover one cannot rule out that the union of the E_n includes all degree- d polynomials defined over K . Indeed, Odoni makes the following tentative conjecture, which is a special case of [35, Conjecture 7.5]:

Conjecture 2.2 (Odoni). *For each $d \geq 2$, there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree d with $G_\infty(f) = \text{Aut}(T_\infty)$.*

This conjecture remains open for all $d \geq 3$. While Theorem 2.1 does not answer Question 1.1 (a) or (b) for any single polynomial, it does offer evidence that in the absence of some sort of arithmetic coincidence one expects to find $G_\infty(f) = \text{Aut}(T_\infty)$.

Quadratic polynomials, as they do often in questions related to dynamics, furnished the first realm where it became possible to answer Question 1.1 in certain cases, though

much remains unknown. As noted in the introduction, Odoni showed in [36] that $G_\infty(f) = \text{Aut}(T_\infty)$ in the case $K = \mathbb{Q}$, $f(x) = x^2 - x + 1$. Moreover, in [37, Section 4], he responded to a question of J. McKay by giving a powerful algorithm for deciding whether $G_n(f) = \text{Aut}(T_n)$ for $f(x) = x^2 + 1$. J. Cremona [5] used this algorithm² to verify the assertion for n up to $5 \cdot 10^7$. Note that for $n = 5 \cdot 10^7$,

$$\log_2 |\text{Aut}(T_n)| = 32^{10000000} - 1,$$

showing that Odoni's method goes far beyond what brute force computation could allow. M. Stoll [50] then furnished a clever trick to show that Odoni's algorithm works for all n , and generalized the result to many other cases:

Theorem 2.3 ([50]). *Let $K = \mathbb{Q}$ and $f(x) = x^2 + k \in \mathbb{Z}[x]$, where $-k$ is not a square, and one of the following holds:*

- $k > 0, k \equiv 1 \pmod{4}$
- $k > 0, k \equiv 2 \pmod{4}$
- $k < 0, k \equiv 0 \pmod{4}$

Then $G_\infty(f) = \text{Aut}(T_\infty)$.

Interestingly, there is no way to extend Stoll's method to all other cases where $-k$ is not a square. For instance, when $k = 3$, one finds that $[\text{Aut}(T_3) : G_3(f)] = 2$, even though the third iterate of $f(x) = x^2 + 3$ is irreducible. As we will see shortly, this arises from the curious fact that both $f^2(0)$ and $f^3(0)$ have large square factors. W. Hindes [16] has recently shown that $k = 3$ is the only integer to exhibit this particular degeneracy, thereby answering a question of the author. In [15], Hindes conjectures that $[\text{Aut}(T_\infty) : G_\infty(f)] = 2$, using an updated form of Hall's conjecture (involving the size of the integral points on the Mordell curves $y^2 = x^3 + A$). However, at present it is not known whether $[\text{Aut}(T_\infty) : G_\infty(f)]$ is even finite.

In addition to these polynomial cases, there is at present just one more rational function $\phi \in \mathbb{Q}(x)$ for which it is known that $G_\infty(f) = \text{Aut}(T_\infty)$ for $K = \mathbb{Q}$, namely

$$(6) \quad \phi(x) = \frac{1 + 3x^2}{1 - 4x - x^2}.$$

See [25, Theorem 1.2]. This particular function has a critical point at $x = 1$ that lies in a two-cycle, similar to a polynomial's fixed critical point at infinity. We shall have more to say at the end of Section 2.2 about the additional fortuitous properties of ϕ that allow for this result. In [20, Theorem 3.2], it is shown using a minor variation of Stoll's technique that we have $G_\infty(f) = \text{Aut}(T_\infty)$ for $f(x) = x^2 + t$, provided that K has characteristic $p \equiv 3 \pmod{4}$. It would be interesting to know if the same results holds when K has arbitrary odd characteristic.

²According to Cremona, his ability to push the calculation so far relied in part on a computer bug. While running his program on a powerful computer cluster at the University of Bath, a Friday night glitch effectively killed all the processes but his, allowing his program to hog the machine all weekend.

In a handful of additional cases it is known that $[\text{Aut}(T_\infty) : G_\infty(f)] < \infty$. The next result follows from work in [22]; see the remark following the proof of Theorem 1.1 of [22]. We recall some definitions:

- A rational map is *post-critically finite* if the forward orbit of each of its critical points is finite (see Section 3.1 for more about such maps).
- A point α is *periodic* under a rational map ϕ if $\phi^n(\alpha) = \alpha$ for some $n \geq 1$.
- A point α is *pre-periodic* under ϕ if $\phi^n(\alpha) = \phi^m(\alpha)$ for some $n > m \geq 0$, where we set $\phi^0(\alpha) = \alpha$.
- A point α is *strictly pre-periodic* under ϕ if it is pre-periodic but not periodic.

Theorem 2.4 ([22]). *Let $K = \mathbb{Q}$, and $f \in \mathbb{Z}[x]$ be monic and quadratic. Suppose f is not post-critically finite, and 0 is strictly pre-periodic under f . Assume further that all iterates of f are irreducible over \mathbb{Q} . Then G_∞ has finite index in $\text{Aut}(T_\infty)$.*

The irreducibility hypothesis in Theorem 2.4 is essential, as will be shown in Section 2.2. It is tempting to replace it with the condition that the number of irreducible factors of $f^n(x)$ be bounded independently of n , but at present no proof is known with this weaker condition. As an illustration, suppose that $f(x)$ splits into two linear factors $g_1(x)g_2(x)$, but $g_1(f^n(x))$ and $g_2(f^n(x))$ are irreducible for all $n \geq 1$ (such statements are often provable; see for example the discussion of eventual stability in Section 5 and [22, Proposition 4.5]). Even if one computes the Galois groups of $g_1(f^{n-1}(x))$ and $g_2(f^{n-1}(x))$, which is also often possible, one must then address the possibility that these groups do not operate independently on the roots of $f^n(x)$. In other words, the splitting fields of $g_1(f^{n-1}(x))$ and $g_2(f^{n-1}(x))$ may have non-trivial intersection. Getting a handle on this intersection appears to be a difficult problem.

In [22], it is shown that Theorem 2.4 applies to these families of maps:

- (1) $f(x) = x^2 - kx + k$ for all $k \in \mathbb{Z} \setminus \{-2, 0, 2, 4\}$.
- (2) $f(x) = x^2 + kx - 1$ for all $k \in \mathbb{Z} \setminus \{-1, 0, 2\}$.

In family (1), the exceptions $k = -2, 0, 2$ give polynomials that are post-critically finite, while for $k = 4$ we obtain the reducible polynomial $g(x) = x^2 - 4x + 4$. In [22, Proposition 4.6] it is shown that $g^n(x)$ is the square of an irreducible polynomial for all $n \geq 1$, and this is enough to allow for a density zero result for orbits of this map (see Section 4). However, at present no proof that $[\text{Aut}(T_\infty) : G_\infty(g)] < \infty$ is known. In family (2), $k = 0, 2$ give post-critically finite polynomials, while for $k = -1$ the polynomial $h(x) = x^2 - x - 1$ has the curious property that $h^2(x)$ is irreducible, but $h^3(x)$ factors as the product of two irreducible quartics. This furnishes the same obstacles to showing $[\text{Aut}(T_\infty) : G_\infty(h)] < \infty$ as in the $k = 4$ case for family (1). Interestingly, $h(x)$ is the minimal polynomial of the golden mean. No one knows whether special properties of the golden mean are related to the highly unusual factorization of $h^3(x)$.

Recently, C. Gratton, K. Nguyen, and T. Tucker [12] proved another important result in this area, giving evidence that one should expect $[\text{Aut}(T_\infty) : G_\infty(f)] < \infty$ when f is a quadratic polynomial.

Theorem 2.5 ([12]). *Let $K = \mathbb{Q}$, and let $f(x) \in \mathbb{Z}[x]$ be monic, quadratic, and not post-critically finite. Assume that all iterates of f are irreducible. Then the ABC conjecture implies $[\text{Aut}(T_\infty) : G_\infty(f)] < \infty$.*

Theorem 2.5 is a slightly generalized form of [12, Proposition 6.1]; we explain below how it follows from the main results of [12]. With minimal difficulty, one can generalize Theorem 2.5 so that the field of definition of f is a number field. However, as in Theorem 2.4, the irreducibility hypothesis on the iterates of f is essential. Thus we are left with the surprising state of affairs that establishing the irreducibility of iterates of f is the key step; once that is known, it is an easier path to prove the Galois groups of such iterates are large. We will see this theme again when examining rational functions with non-trivial automorphisms in Section 3.4. See Section 5 for more on the question of irreducibility of iterates.

2.2. A sketch of the method. Let us briefly sketch the method underlying the results of Section 2.1, restricting ourselves to the situation where $K = \mathbb{Q}$ and $f \in \mathbb{Z}[x]$ is a monic, quadratic polynomial. This case is of sufficient simplicity to highlight the essential elements of the method, but of sufficient depth to require much of their full strength. We denote by c the critical point of f , and assume that c does not lie in $f^{-n}(0)$ for any $n \geq 0$, thereby ensuring that $f^n(x)$ has 2^n distinct roots. Let K_n denote the field $\mathbb{Q}(f^{-n}(0))$, so that $G_n = \text{Gal}(K_n/\mathbb{Q})$, and denote by H_n the Galois group of the relative extension K_n/K_{n-1} . One may roughly summarize the method as follows: H_n is as large as possible provided that a prime ramifies in the extension K_n/K that did not already ramify in K_{n-1}/K . Candidates for this newly ramified prime are found only among primes dividing $f^n(c)$ that do not divide $f^i(c)$ for $i < n$, and thus we must study the arithmetic of the orbit of c under f . Sufficient knowledge of this arithmetic is available only in the cases covered by the results in Section 2.1.

Note that K_n is obtained from K_{n-1} by adjoining the roots of $f(x) - \beta_i$, where $\beta_1, \dots, \beta_{2^{n-1}}$ are the roots of $f^{n-1}(x)$. This is the same as adjoining the 2^{n-1} square roots $\sqrt{\delta_i}$, where

$$\delta_i := \text{Disc}(f(x) - \beta_i),$$

and thus K_n is a 2-Kummer extension of K_{n-1} , and we have an injection $H_n \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}$. This injection is also apparent from our identification of G_n with a subgroup of $\text{Aut}(T_n)$, since H_n must lie in the kernel of the restriction mapping $\text{Aut}(T_n) \rightarrow \text{Aut}(T_{n-1})$, which is generated by the transpositions swapping a pair of vertices at level n that are both connected to the same vertex at level $n-1$. We thus refer to H_n as *maximal* when

$$H_n = \ker(\text{Aut}(T_n) \rightarrow \text{Aut}(T_{n-1})), \quad \text{or equivalently } H_n \cong (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}.$$

Clearly we have $G_n(f) = \text{Aut}(T_n)$ if and only if H_i is maximal for $i = 1, 2, \dots, n$.

Using Kummer theory (e.g. [27, Section VI.8]), $[K_n : K_{n-1}]$ is the order of the group D generated by the classes of the δ_i in K_{n-1}^*/K_{n-1}^{*2} , where K_{n-1}^{*2} denotes the non-zero squares in K_{n-1} . We have

$$\#D = \frac{2^{2^{n-1}}}{\#V}, \text{ where } V = \{(e_1, \dots, e_{2^{n-1}}) \in \mathbb{F}_2^{2^{n-1}} : \prod_j \delta_j^{e_j} \in K_{n-1}^{*2}\}.$$

Thus V is the group of multiplicative relations among the δ_i , up to squares. One sees easily that V is an \mathbb{F}_2 -vector space, and that the action of G_{n-1} on the δ_i gives an action of G_{n-1} on V as linear transformations. It follows that V is an $\mathbb{F}_2[G_{n-1}]$ -module. Perhaps surprisingly, one can show that if V is non-trivial, then it must contain the element $(1, \dots, 1)$ *provided that the action of G_{n-1} on the δ_i is transitive*, or equivalently that $f^{n-1}(x)$ is irreducible. One begins by showing that if $V \neq 0$, then the submodule $V^{G_{n-1}}$ of G_{n-1} -invariant elements is non-trivial, a result that relies on G_{n-1} being a 2-group (see [50, Lemma 1.6]). The transitivity of the action of G_{n-1} on the δ_i then assures that if $V^{G_{n-1}}$ is non-empty, then it must contain $(1, \dots, 1)$.

Now $(1, \dots, 1) \in V$ if and only if

$$(7) \quad \prod_{i=1}^{2^{n-1}} \text{Disc}(f(x) - \beta_i)$$

is a square in K_{n-1} . But $\text{Disc}(f(x) - \beta_i) = -4(b - \beta_i)$, where we write $f(x) = (x - c)^2 + b$. As the β_i vary over all roots of $f^{n-1}(x)$, the product in (7) is $(-4)^{2^{n-1}} f^{n-1}(b)$. But $f^{n-1}(b) = f^{n-1}(f(c)) = f^n(c)$, and hence (7) is a square in K_{n-1} if and only if $f^n(c)$ is a square in K_{n-1} .

To sum up, assuming that $f^{n-1}(x)$ is irreducible, we've shown

$$(8) \quad [K_n : K_{n-1}] = 2^{2^{n-1}} \text{ if and only if } f^n(c) \text{ is not a square in } K_{n-1}.$$

This key result has generalizations in a variety of directions. An easy and direct generalization is to replace the ground field \mathbb{Q} with any number field K (and allow K to be the field of definition for f). For a similarly small price, one can let G_n be the Galois group over K of polynomials of the form $g(f^n(x))$, where f is still quadratic and g is arbitrary [22, Lemma 3.2]. When f is allowed to be a quadratic rational function, the only known result becomes significantly more complicated: the condition is essentially that the numerator of $f^n(c_1)f^n(c_2)$ not be a square in K_{n-1} , where c_1 and c_2 are the two critical points of f [25, Theorem 3.7].

To apply these results in any of the above settings requires showing that a given element of K_{n-1} is not a square in K_{n-1} , a problem which seems difficult at first blush since K_{n-1} is generally a huge-degree extension. However, the element in question (e. g. $f^n(c)$) is in fact an element of the ground field, which makes things considerably easier. Let us return to the setting where $f(x)$ is a monic, quadratic polynomial defined over \mathbb{Z} , and our ground field is \mathbb{Q} . If $f^n(c)$ is divisible to an odd power by a prime

p , then $f^n(c)$ can only become a square in K_{n-1} if p ramifies in K_{n-1} . The iterative nature of the extensions K_{n-1} allows us to explicitly describe a set of primes that must include all those that ramify in K_{n-1} . More specifically, a calculation with resultants gives

$$(9) \quad \text{Disc}(f^k) = \pm 2^{2^k} (\text{Disc}(f^{k-1}))^2 f^k(c)$$

for all $k \geq 1$ [22, Lemma 2.6 and discussion following]. The appearance of $f^k(c)$ in (9) is actually rather intuitive: f^k has a multiple root modulo an odd prime p only when f^{k-1} already had such a root, or a critical point appears in $f^{-k}(0)$ modulo p . The latter condition is equivalent to $f^k(c) \equiv 0 \pmod{p}$, or $p \mid f^k(c)$. Because K_{n-1} is the splitting field of $f^{n-1}(x)$ over \mathbb{Q} , the true discriminant of the extension K_{n-1}/\mathbb{Q} divides $\text{Disc}(f^{n-1})$. A simple induction using (9) gives that the only primes dividing $\text{Disc}(f^{n-1})$ are those dividing one of $2, f(c), f^2(c), \dots, f^{n-1}(c)$. We at last obtain the criterion that gives rise to nearly all of the results of Section 2.1:

Theorem 2.6 ([22]). *Let $f \in \mathbb{Z}[x]$ be monic and quadratic with critical point c , and let K_n and H_n be defined as on p. 8. Assume that $f^{n-1}(x)$ is irreducible and there exists an odd prime $p \in \mathbb{Z}$ whose p -adic valuation v_p satisfies $v_p(f^n(c))$ odd and $v_p(f^i(c)) = 0$ for $i = 1, 2, \dots, n-1$. Then H_n is maximal.*

In other words, assuming that $f^{n-1}(x)$ is irreducible, the element $f^n(c)$ of the sequence $(f^i(c))_{i \geq 1}$ must have a primitive prime divisor appearing to odd multiplicity. In terms of ramification, Theorem 2.6 requires that a “new” prime p ramify in K_n (that is, one that has not already ramified in K_i for $i < n$). This result has generalizations in the same directions as those of (8); see [22, Theorem 3.3] and [25, Corollary 3.8].

The hypothesis that $f^{n-1}(x)$ be irreducible is essential in Theorem 2.6. Fortunately, in many cases one finds that *all* iterates of $f(x)$ are irreducible, a fact we discuss further in Section 5. Indeed, to show this it is enough to prove that f is irreducible and the orbit of c under f (called the *critical orbit* of f) contains no squares (see Theorem 5.1). This fact, together with Theorem 2.6, shows that the nature of $G_\infty(f)$ depends crucially (critically, even) on arithmetic properties of the critical orbit of f . This makes for a striking analogy with complex and real dynamics, where analytic properties of the critical orbit of a quadratic polynomial have been shown to determine fundamental dynamical behavior of the polynomial. For instance, if $f \in \mathbb{C}[z]$ is quadratic, then membership in the Mandelbrot set – and equivalently the connectedness of the filled Julia set of f – is determined by whether the critical orbit remains bounded [9, Section 3.8].

To apply Theorem 2.6 requires getting a handle on the primes dividing elements in the critical orbit of f , which is generally very difficult. One may obtain some tantalizing results, however. In Section 4 we will see that it is vital to be able to show that H_n is maximal for infinitely many n . We invite the reader to show that in the setting of Theorem 2.6 there are infinitely many n such that $f^n(c)$ has a primitive prime

divisor³; unfortunately one cannot guarantee that the first appearance of such a prime in the sequence $(f^i(c))_{i \geq 1}$ is to odd multiplicity. Similarly, one can show that there must be infinitely many primes p dividing at least one term $f^n(c)$ to odd multiplicity; unfortunately, one cannot guarantee that when they do so their appearance is primitive.

The ABC conjecture rescues us from this predicament, as shown in [12, Theorem 1.2]: it implies that for all but finitely many n , there is a primitive prime divisor of $f^n(c)$ appearing to multiplicity 1 (note that in our situation, $f(x)$ is dynamically ramified in the terminology of [12] if and only if $f(x) = x^2$). Thus Theorem 2.5 is an immediate corollary of [12, Theorem 1.2]. Interestingly, J. Silverman [45] has shown that in higher dimensions, Vojta's conjecture implies a result on primitive prime divisors similar to [12, Theorem 1.2]. However, as the Galois theory of preimages in the higher-dimensional setting is all but nonexistent at present, the Galois-theoretic implications of Silverman's result remain unclear.

In special circumstances, we may even obtain unconditional results. When $f(x) = x^2 + k$, an easy application of Theorem 5.1 shows that all iterates of f are irreducible provided that $-k$ is not a square. The lack of linear term in f ensures that the resulting critical orbit $(f^i(0))_{i \geq 1}$ satisfies a powerful property known as *rigid divisibility* [22, p. 524]. Namely, setting $a_n = f^n(c)$ we have:

- $v_p(a_n) > 0$ implies $v_p(a_{mn}) = v_p(a_n)$ for all $m \geq 1$, and
- $p^e \mid a_n$ and $p^e \mid a_m$ implies $p^e \mid a_{\gcd(m,n)}$.

One then defines a “primitive part” b_n of each a_n by setting $b_n = \prod_{d \mid n} a_n^{\mu(n/d)}$, where μ denotes the Möbius function, and shows that the b_n are pairwise relatively prime. By Theorem 2.6, to prove that H_n is maximal then only requires showing that b_n is not a unit times a square. This is Odoni's criterion, used by Cremona in [5] and by Stoll to prove Theorem 2.3. We now may shed some light on the case of $f(x) = x^2 + 3$: we have $f^2(0) = 2^2 \cdot 3$, and $f^3(0) = 7^2 \cdot 3$, whence $b_2 = 2^2$ and $b_3 = 7^2$. Note that $f^2(0)$ is not a square in $K_1 = \mathbb{Q}(\sqrt{-3})$, and hence $G_2(f) = \text{Aut}(T_2)$ by (8), but $f^3(0)$ is a square in $K_2 = \mathbb{Q}(f^{-2}(0))$, and hence $G_3(f) \neq \text{Aut}(T_3)$.

Another favorable case occurs when f maps 0 into a cycle not containing 0 (or in other words, 0 is strictly pre-periodic under f). Then we have a finite set R consisting of all primes dividing at least one of the elements in the orbit of 0. If p is not such a prime, then $p \mid f^n(c)$ implies $f^{m+n}(c) \equiv f^m(f^n(c)) \equiv f^m(0) \not\equiv 0 \pmod{p}$ for any $m \geq 1$, and hence p divides at most one element of the critical orbit of f . An extreme example of this situation comes from the polynomial $f(x) = x^2 - x + 1$ considered by Odoni in [36]. Here f sends 0 to the fixed point 1, and thus R is empty and the elements of the critical orbit (considered as belonging to $\mathbb{Z}[\frac{1}{2}]$) are pairwise relatively prime. To show $G_\infty(f) = \text{Aut}(T_\infty)$ via Theorem 2.6, the challenge is then to show that $f^n(c)$ is not a square for any $n \geq 1$, which proves surprisingly difficult [36, p. 3].

³or you can take the easy way out and look at [22, Theorem 6.1].

In the more general situation when 0 is pre-periodic under f , to apply Theorem 2.6 it suffices to show that $f^n(c)$ is not a square times a (possibly empty) product of primes in R . One may appeal to Siegel's theorem to achieve this, for the price of excluding a finite set of n . Indeed, if $f^n(c)$ is r times a square, for some product r of primes in R , then the curve $ry^2 = f(f(x))$ has an S -integral point with $x = f^{n-2}(c)$ (here S is empty if $c \in \mathbb{Z}$ and $S = \{2\}$ if $c \notin \mathbb{Z}$). But there can be only finitely many such points, for each of the finitely many choices of r . This establishes Theorem 2.4.

Finally, let us return to the rational function ϕ given in (6). As noted on p. 6, ϕ has a critical point at $x = 1$ that lies in a two-cycle, making ϕ similar to a polynomial. Moreover, ϕ sends 0 into the two-cycle $1 \rightarrow -1 \rightarrow 1$, ensuring that we are in the situation of the previous two paragraphs, and even better with $R = \emptyset$. It follows that any odd prime divides the numerator of at most one term of the wandering critical orbit $\{\phi^n(-1/3) : n \geq 1\}$, and the same is true of the sequence $(a_n) := (p_n(-1/3)p_n(1) : n \geq 1)$, where $p_n(x)$ is essentially the numerator of $\phi^n(x)$ (see [25, Section 2] for a precise definition). The numbers $p_n(-1/3)p_n(1)$ play the role of $f^n(c)$ in Theorem 2.6 (see [25, Corollary 3.8]), though in Theorem 2.6 we required that the desired prime p be odd, and here we require it to be odd and not equal to 3. By reducing modulo 5, one shows that no element of (a_n) is plus or minus a square. Hence each element of (a_n) is divisible by some prime to odd multiplicity, and if this prime is not two or three then its appearance is primitive and we may apply the equivalent of Theorem 2.6. The proof that $[\text{Aut}(T_\infty) : G_\infty(\phi)] < \infty$ thus finishes with a calculation showing the evenness of the 2-adic and 3-adic valuation of all terms of (a_n) . See the end of Section 3 of [25] for the full details.

A major obstacle to extending these methods to higher-degree polynomials is that in (9) and Theorem 2.6, the appearance of $f^n(c)$ is replaced by $\prod f^n(c)$, where the product is over all critical points c of ϕ . There appears to be no easy way to rule out arithmetic interactions among the elements of several critical orbits.

3. THE IMAGE OF ρ : EXCEPTIONAL CASES

In light of the results of Section 2, and especially Theorems 2.1 and 2.5, it is tempting to conjecture that $[\text{Aut}(T_\infty) : G_\infty(\phi)] < \infty$ unless there is a structural reason this cannot occur. In the setting of Galois representations attached to elliptic curves, the structural reason is the curve having complex multiplication, and Serre's theorem (see (4)) shows that this is the only exception. In our case, one encounters a profusion of structural reasons, four of which we discuss in this section. Unfortunately, there does not seem to be a general principle to suggest that these four exhaust all possibilities, and correspondingly it seems impossible at present to make a convincing finite-index conjecture. However, enough results and examples have now been accumulated for quadratic ϕ that we pose a conjecture in this case: see Conjecture 3.11.

We begin with examples of four rational functions for which $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is infinite, each illustrating a class of exceptions to any finite index conjecture:

- (a) $\phi(x) = x^2 - 2$
- (b) $\phi(x) = x^3 + 2$
- (c) $\phi(x) = x^2 + x$
- (d) $\phi(x) = (x^2 + 1)/x$

In (a), ϕ is post-critically finite, which we recall means that the forward orbit of each critical point of ϕ is finite. In (b), ϕ is not post-critically finite, but has overlapping critical orbits: 0 is a point of multiplicity 3, which may be thought of as two co-incident critical orbits. In (c), the root 0 of T_∞ is periodic under ϕ . In (d), ϕ commutes with a non-trivial Möbius transformation.

In cases (a) and (b), the impediments to $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ being finite are geometric, in that they are invariant under changing the root of the tree T_∞ . Cases (c) and (d), on the other hand, are arithmetic in that they depend on the root of T_∞ having special algebraic properties. In Section 3.1 we discuss the case where ϕ is post-critically finite, and we show $G_\infty(\phi)$ has infinite index in $\text{Aut}(T_\infty)$ for such maps. We also discuss what is known about the group G^{arith} obtained by replacing the root 0 of T_∞ by an element t that is transcendental over K , and working over the ground field $K(t)$. This group gives an over-group for $G_\infty(\phi)$, and the latter is obtained by the specialization $t = 0$. Cases (b), (c), and (d) are discussed in Sections 3.2, 3.3, and 3.4, respectively.

3.1. Post-critically finite rational functions. The discussion just before and after Theorem 2.6 shows how the arithmetic of the forward orbit of the critical point of a quadratic polynomial ϕ plays a key role in the study of $G_\infty(\phi)$. A similar relationship holds for more general maps, as we now explain. Let $K_n = K(\phi^{-n}(0))$, and consider the question of which primes of K ramify in K_n , and in particular which ramify in K_n/K but not in K_{n-1}/K . Thanks to several generalizations of the discriminant formula (9), it is known that these primes must belong to a very restricted set. First W. Aitken, F. Hajir, and C. Maire gave a generalization to polynomials of arbitrary degree [2], and recently J. Cullinan and Hajir [6] as well as the author and M. Manes [25, Theorem 3.2] have produced further generalizations to rational functions. In each case, the formulae show that the only primes of K that can ramify in the extensions K_n/K are those dividing $\phi^i(c)$ for some critical point c of ϕ (aside from a finite set of primes that does not grow with n , such as the primes dividing the resultant of ϕ).

Now a generic rational function $\phi \in K(x)$ of degree d has $2d - 2$ distinct critical points, all with infinite and non-overlapping orbits. This allows for the collection of primes dividing at least one element of the form $\phi^i(c)$ to be large, and thus there are many possibilities for primes ramifying in K_n . At the extreme of non-generic behavior are the post-critically finite rational functions, which have only a *finite set* of primes, independent of n , that can ramify in any K_n (this is among the main results in [2] and [6]). In other words, the extension $K_\infty := \bigcup_{n=1}^\infty K_n$ is a finitely ramified extension of K .

Because the inertia subgroups at the ramified primes generate $\text{Gal}(K_\infty/U_\infty)$, where U_∞ is the (presumably small) maximal unramified sub-extension of K_∞ , we should generally expect $G_\infty(\phi)$ to be a small subgroup of $\text{Aut}(T_\infty)$ when ϕ is post-critically finite. We now give a result in this direction, whose proof evolved through discussions between the author and R. Pink.

Theorem 3.1. *Suppose that K is a global field of characteristic 0 or $> d$, and let $\phi \in K(x)$ be a post-critically finite map of degree d . Then $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is infinite.*

Proof. We first argue that if $H \leq \text{Aut}(T_\infty)$ is (topologically) generated by the conjugacy classes of finitely many elements, then $[\text{Aut}(T_\infty) : H]$ is infinite. A standard result in group theory is that $\text{Aut}(T_n) \cong S_d^{(n)}$, where the latter group is the n -fold iterated wreath product of the symmetric group S_d on d letters. Moreover, the abelianization of $\text{Aut}(T_n)$ is given by

$$(10) \quad \text{Aut}(T_n)^{\text{ab}} \cong ((S_d)^{\text{ab}})^n \cong (\mathbb{Z}/2\mathbb{Z})^n,$$

where the first isomorphism follows from the fact that the abelianization of the wreath product of groups G_1 and G_2 is $G_1^{\text{ab}} \times G_2^{\text{ab}}$ [8, p. 215]. Denote by

$$\tau : \text{Aut}(T_\infty) \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$$

the homomorphism obtained from (10). By our assumption about H , the group $\tau(H)$ is finitely generated, and hence finite. Therefore $[\tau(\text{Aut}(T_\infty)) : \tau(H)]$ is infinite, whence $[\text{Aut}(T_\infty) : H]$ is infinite as well.

By the main result of [6], the extension K_∞ of K is unramified outside a finite set S of places of K . Assume first that K is a number field. It follows from a result of Ihara (see [34, Theorem 10.2.5]) that the Galois group $G_{K,S}$ of the *maximal* extension of K unramified outside S is (topologically) generated by the conjugacy classes of finitely many elements. As $G_\infty(\phi)$ is a quotient of this group, it shares the same property. When K is a global function field, the group $G_{K,S}$ may be quite complicated in general. However, our assumption that K has characteristic $> d$ implies that the ramification in K_∞ is tame, and hence $G_\infty(\phi)$ is a quotient of the maximal tamely ramified extension of K that is unramified outside S . This latter group is (topologically) finitely generated [34, Corollary 10.1.6], and hence so is $G_\infty(\phi)$. In particular, $G_\infty(\phi)$ is (topologically) generated by the conjugacy classes of finitely many elements. \square

Let us now discuss the group G^{arith} , first alluded to on p. 13. Let t be transcendental over K , and consider the action of the absolute Galois group of $K(t)$ on the tree $T_\infty(t) \subset \overline{K(t)}$ of iterated pre-images of t under ϕ . The image of this action is G^{arith} , also known as the (*profinite*) *arithmetic iterated monodromy group* of ϕ . Note that $\text{Aut}(T_\infty(t))$ and $\text{Aut}(T_\infty)$ are naturally isomorphic, so we may think of $G_\infty(\phi)$ as the subgroup of G^{arith} obtained via the specialization $t = 0$. Thus in a loose sense G^{arith} gives the group one expects $G_\infty(\phi)$ to be under the choice of a generic root of T_∞ .

As G^{arith} is the Galois group of the extension $K_{\infty,t} := \bigcup_{n \geq 1} K(\phi^{-n}(t))$ over $K(t)$, it has a normal subgroup G^{geom} corresponding to the subfield $L(t)$, where $L := \overline{K} \cap K_{\infty,t}$ is the maximal constant field extension contained in $K_{\infty,t}$. This gives an exact sequence

$$(11) \quad 1 \rightarrow G^{\text{geom}} \rightarrow G^{\text{arith}} \rightarrow \text{Gal}(L/K) \rightarrow 1,$$

The primes of $L(t)$ over which $K_{\infty,t}$ is ramified correspond to the ramification points of the covers $\phi^n : \mathbb{P}^1 \rightarrow \mathbb{P}^1$, for $n = 1, 2, \dots$. One easily sees that this is the same as the post-critical set C of ϕ , namely the set $\{\phi^n(c) : n \geq 1 \text{ and } c \text{ is a critical point of } \phi\}$. In the case where the characteristic of K is either 0 or greater than the degree d of ϕ , the extension $K_{\infty,t}$ has only tame ramification over $L(t)$, and hence G^{geom} is a quotient of the tame fundamental group of $\mathbb{P}_{\overline{K}}^1 \setminus C$. When ϕ is post-critically finite, the resulting finiteness of C implies that this tame fundamental group is (topologically) finitely generated, and hence so is G^{geom} . Moreover, the inertia subgroup corresponding to each point in C is pro-cyclic, and one may hope to give an explicit description of the action of its generator on $T_{\infty}(t)$. Note that the group G^{geom} does not change under extension of L , and thus when K is a number field we may calculate G^{geom} over \mathbb{C} . In this case, G^{geom} is given by the closure of the image of the topological fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus C)$ in $\text{Aut}(T_{\infty}(t))$; this image is known as the *iterated monodromy group* of ϕ . (We ignore the base point of the fundamental group, as it only affects the resulting subgroup of $\text{Aut}(T_{\infty}(t))$ by a conjugation.) Then the action of inertial generators may be calculated explicitly using ϕ -lifts of certain loops in \mathbb{C} , and one obtains a beautiful description of these generators in terms of a finite automaton. See for instance [32, 33] for more on this theory. When K is a field of characteristic $> d$ and ϕ is post-critically finite, one may hope that inertial generators of the action of G^{geom} on $T_{\infty}(t)$ may still be given by the states of a finite automaton. However, this is only known at present in the case where ϕ is a quadratic rational function [39].

What, then, may be said about the group G^{arith} ? Unfortunately, the extension L in (11) remains mysterious in general, particularly in the case where ϕ is post-critically finite. An outstanding contribution of [40] is the computation of L when ϕ is a post-critically finite quadratic polynomial defined over a general field K . In particular, $[L : K]$ is finite when the orbit of the critical point of ϕ is pre-periodic and the post-critical set has at least 3 elements. Otherwise, $[L : K]$ is infinite. In either case, the extension L/K is contained in the extension of K generated by the primitive (2^n) th roots of unity for $n = 1, 2, \dots$. It follows that G^{arith} is a topologically finitely generated subgroup of $\text{Aut}(T_{\infty}(t))$. When ϕ is a quadratic rational function that is *not* post-critically finite, then G^{arith} is completely determined in [41]; see the discussion following Question 3.3. In Section 3.2 we discuss G^{arith} and G^{geom} when ϕ is a non-post-critically finite map of the form $x^d + b$.

To close this subsection, we mention that it is a very interesting question, both when ϕ is post-critically finite and in general, to determine whether there are special properties of the conjugacy classes in $G_{\infty}(\phi)$ of Frobenius elements at the various primes

of K . In the general case, the author and N. Boston have made some conjectures; we refer the reader to [3] for details. When $G_\infty(\phi)$ is a small subgroup of $\text{Aut}(T)$, the possibility arises that special properties of the Frobenius conjugacy classes could be related to the structure of $G_\infty(\phi)$. To state this question more precisely, we note that the *Hausdorff dimension* of $G_\infty(\phi)$ is by definition

$$\liminf_{n \rightarrow \infty} \frac{\log \#G_n(\phi)}{\log \#\text{Aut}(T_n)}.$$

Question 3.2. Suppose that the Hausdorff dimension of $G_\infty(\phi)$ is < 1 . How does the structure of $G_\infty(\phi)$ relate to properties of Frobenius conjugacy classes?

3.2. Rational functions with overlapping critical orbits. Post-critically finite maps represent an extreme among non-generic critical configurations, and it is natural to ask whether less extreme configurations also lead to restrictions on $G_\infty(\phi)$. A first remark is that even the seemingly severe restriction that ϕ be a polynomial, i.e. have a totally ramified fixed critical point, does not a priori impose restrictions on $G_\infty(\phi)$, as evidenced by Theorem 2.1. Similarly, the quadratic map in (6) has one wandering critical point and one in a 2-cycle, yet has $G_\infty(\phi) = \text{Aut}(T_\infty)$.

On the other hand, let us consider maps of the form $\phi(x) = x^d + b$, where $d \geq 2$ and $b \in K$ is such that 0 has infinite forward orbit under ϕ (or equivalently, ϕ is not post-critically finite). The fact that ϕ has only a single critical orbit besides the fixed point at infinity is enough to force $G_\infty(\phi)$ to be a very small subgroup of $\text{Aut}(T_\infty)$. Indeed, the extension K_{n+1}/K_n is obtained by adjoining the d th roots of d^n elements, and hence for $n \geq 1$ has degree at most d^{d^n} (since K_n contains a primitive d th root of unity when $n \geq 1$). But the kernel of the restriction $\text{Aut}(T_{n+1}) \rightarrow \text{Aut}(T_n)$ is isomorphic to $(S_d)^{d^n}$, and thus has order $(d!)^{d^n}$. It follows that the Hausdorff dimension of $G_\infty(\phi)$ is at most $(\log d)/(\log(d!))$, and in particular, $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is infinite for $d \geq 3$. It follows from Stirling's formula that $(\log d)/(\log(d!))$ is roughly $1/d$. More precisely,

$$\frac{\log d}{\log d!} = \left(d - \frac{d}{\ln d} + O(1) \right)^{-1}.$$

For a more thorough examination of the nature of $G_\infty(\phi)$ in this case, see [14]. We remark that it is reasonable to expect that the image of G^{geom} in $\text{Aut}(T_n(t))$ is isomorphic to the n -fold wreath product of $\mathbb{Z}/d\mathbb{Z}$, for each $n \geq 1$. In this case, the extension L in (11) is simply $K(\zeta_d)$, and hence $G^{\text{arith}}/G^{\text{geom}}$ has order at most $d - 1$.

In light of the preceding analysis, it seems likely that $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is infinite whenever ϕ has degree at least 3 and only a single wandering critical orbit. More generally, we pose this question:

Question 3.3. Suppose that ϕ is not post-critically finite. What restrictions on the critical orbits of ϕ ensure that $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is infinite?

In the case where ϕ is quadratic, Question 3.3 has been resolved by R. Pink [40] as follows. If γ_1 and γ_2 are the two critical points of ϕ , and there is a relation of the form

$$(12) \quad \phi^{r+1}(\gamma_1) = \phi^{r+1}(\gamma_2) \text{ for some } r \geq 1,$$

then G^{arith} has Hausdorff dimension $1 - 2^{-r}$ in $\text{Aut}(T_\infty(t))$, and in particular $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is infinite. Moreover, $G^{\text{arith}}/G^{\text{geom}}$ has order 1 or 2. In the absence of a relation of the form given in (12), Theorem 4.8.1(a) of [40] gives

$$(13) \quad G^{\text{arith}} = G^{\text{geom}} = \text{Aut}(T_\infty(t)).$$

Let us give an example of this kind of behavior, which can be found in [40, Example 4.9.5]. Consider the map

$$\phi(x) = \frac{x^2 - a}{x^2 + a},$$

where $a \in \mathbb{Q} \setminus \{0, \pm 1\}$. The critical points of ϕ are 0 and ∞ , and we have $\phi(0) = -1$, $\phi(\infty) = 1$, and $\phi^2(0) = \phi^2(\infty) = (1 - a)/(1 + a)$. Moreover, one checks that the stipulation that $a \notin \{0, \pm 1\}$ implies that ϕ is not conjugate to any of the maps in the list of Manes-Yap [28], and thus is not post-critically finite. Hence G^{arith} is a subgroup of $\text{Aut}(T_\infty(t))$ of Hausdorff dimension $1/2$, and so $G_\infty(\phi)$ has Hausdorff dimension at most $1/2$.

3.3. Rational functions for which 0 is periodic. Let K be a global field, and recall our running assumption that for each $n \geq 1$, the solutions to $\phi^n(x) = 0$ are distinct. Suppose that $\phi^k(0) = 0$ for some $k \geq 1$, so that ϕ has the cycle $0 \mapsto a_1 \mapsto a_2 \cdots \mapsto a_{k-1} \mapsto 0$ in $\mathbb{P}^1(K)$. If we set $a_0 = 0$, then for each $n \geq 1$ we have $a_{r_n} \in \phi^{-n}(0)$, where $n \equiv r_n \pmod k$ and $0 \leq r_n \leq k - 1$. The a_i all lie in K , and hence each set $\phi^{-n}(0)$ contains an element of K , which must be fixed by all elements of $G_n(\phi)$. As $\text{Aut}(T_n)$ acts naturally on the set $\phi^{-n}(0)$, we obtain an injection

$$(14) \quad G_n(\phi) \hookrightarrow \text{Stab}(a_{r_n}),$$

where $\text{Stab}(a_{r_n})$ denotes the stabilizer in $\text{Aut}(T_n)$ of $a_{r_n} \in \phi^{-n}(0)$. Now it's easy to see that $\text{Aut}(T_n)$ acts transitively on $\phi^{-n}(0)$, and hence the orbit of a_{r_n} has size d^n . Thus $[\text{Aut}(T_n) : \text{Stab}(a_{r_n})] = d^n$ by the orbit-stabilizer theorem. Therefore from (14) we have $[\text{Aut}(T_n) : G_n(\phi)] \geq d^n$, and hence $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is infinite. Another way to say this is to note that since $\phi(a_{r_{n+1}}) = a_{r_n}$, restriction gives a natural surjection $\text{Stab}(a_{r_{n+1}}) \rightarrow \text{Stab}(a_{r_n})$, and we may thus define Stab_∞ to be the inverse limit of these stabilizers. Intuitively, Stab_∞ is the stabilizer in $\text{Aut}(T_\infty)$ of a single infinite branch in T_∞ . Note that $[\text{Aut}(T_\infty) : \text{Stab}_\infty] = \infty$, since $[\text{Aut}(T_n) : \text{Stab}(a_{r_n})] = d^n$. Moreover, (14) gives

$$(15) \quad G_\infty(\phi) \hookrightarrow \text{Stab}_\infty.$$

In light of (15), we think of $G_\infty(\phi)$ as a subgroup of Stab_∞ . If there are no other special circumstances forcing $G_\infty(\phi)$ to be smaller than the generic case (such as ϕ

being post-critically finite), then it is reasonable to expect that $[\text{Stab}_\infty : G_\infty(\phi)]$ is finite.

Question 3.4. Let K be a global field and let $\phi \in K(x)$ satisfy $\phi^k(0) = 0$ for some $k \geq 1$. Under what conditions is it possible to prove that $[\text{Stab}_\infty : G_\infty(\phi)]$ is finite?

At present, there is not a single known example of a rational function for which $[\text{Stab}_\infty : G_\infty(\phi)]$ is finite.

We close this subsection by noting that if $\phi^k(0) = 0$, then the number of irreducible factors of the numerator of $\phi^n(x)$ is without bound as n grows. Indeed, one may assume inductively that the numerator of $\phi^{k(n-1)}(x)$ has at least $n-1$ irreducible factors. But then the fact that x divides the numerator of $\phi^k(x)$ implies that the numerator of $\phi^{k(n-1)}(x)$ divides the numerator of $\phi^{kn}(x)$, proving that the latter has at least n irreducible factors. We return to this topic in Section 5.

3.4. Rational functions that commute with non-trivial Möbius transformations. Suppose that $m \in \text{PGL}_2(K)$ satisfies

$$(16) \quad m^{-1} \circ \phi \circ m = \phi \quad \text{and} \quad m(0) = 0.$$

Then m acts on T_∞ since $m(0) = 0$, and the action of $G_\infty(\phi)$ on T_∞ commutes with that of m , since m is defined over K . This is analogous to the Galois action on the Tate module of an elliptic curve commuting with the action of an endomorphism of the curve. Let $A(\phi) \leq \text{Aut}(T_\infty)$ be the subgroup generated by the actions of all $m \in \text{PGL}_2(K)$ satisfying the conditions in (16). Then we obtain an injection

$$(17) \quad G_\infty(\phi) \hookrightarrow C(\phi),$$

where $C(\phi)$ is the centralizer of $A(\phi)$ in $\text{Aut}(T_\infty)$. While $A(\phi)$ must be finite [46], and indeed its group structure is limited by the very few finite subgroups of $\text{PGL}_2(K)$, little is known about $C(\phi)$. In particular:

Conjecture 3.5. *We have $[\text{Aut}(T_\infty) : C(\phi)] = \infty$ when $A(\phi)$ is non-trivial.*

The requirement that $A(\phi)$ be non-trivial is akin to considering an elliptic curve with complex multiplication, though in the latter setting $C(\phi)$ is a Cartan subgroup, which is both a very small subgroup of $\text{GL}(2, \mathbb{Z}_\ell)$, and has the striking property of being nearly abelian. In the dynamical setting, it seems unlikely that $C(\phi)$ is close to abelian, and we will see an example of this in a moment. A seemingly much more difficult issue than studying $C(\phi)$ is to resolve the following:

Question 3.6. Let K be a global field and let $\phi \in K(x)$ satisfy $\#A(\phi) > 1$. Under what conditions is it possible to prove that $[C(\phi) : G_\infty(\phi)]$ is finite?

The only case where these issues have been studied in detail is when ϕ has degree 2 [25]. Let us consider the family

$$(18) \quad \phi(x) = \frac{b(x^2 + 1)}{x} \quad (b \in K).$$

Here $A(\phi)$ is generated by the action of the map $x \rightarrow -x$, unless $b = \pm 1/2$, but in this latter case ϕ is post-critically finite and so fits under the rubric of Section 3.1. The group $C(\phi)$ is studied in [25, Section 4], where it is shown that $C(\phi)$ has Hausdorff dimension $1/2$, and hence $[\text{Aut}(T_\infty) : C(\phi)] = \infty$. In spite of this, $C(\phi)$ has an index-two subgroup that is isomorphic to $\text{Aut}(T_\infty)$ [25, Proposition 4.1], a state of affairs that is made possible by the self-similarity of the tree T_∞ .

Several of the main results of [25] relate to Question 3.6. For simplicity, we state them in the case $K = \mathbb{Q}$.

Theorem 3.7 ([25]). *Let $K = \mathbb{Q}$. There is a density 0 set of primes $S \subset \mathbb{Z}$ such that if $b \in \mathbb{Z}$ is not divisible by any $p \in S$ and $\phi(x) = \frac{b(x^2+1)}{x}$, then $G_\infty(\phi) \cong C(\phi)$.*

In fact the set S is given explicitly: it is the set of primes dividing the numerator of $\phi_1^n(1)$ for some $n \geq 1$, where $\phi_1 = (x^2 + 1)/x$. All $p \in S$ satisfy $p \equiv 1 \pmod{4}$. In particular, the theorem applies to

$$b = 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 31, 33, 37, 39, 43, 47, 49, \dots$$

It would be interesting to obtain a similar result with weaker hypotheses on b , which may well be possible by refining the methods of [25]. Another consequence of the work in [25] is:

Theorem 3.8 ([25]). *Let assumptions and notation be as in Theorem 3.7. Then we have $[C(\phi) : G_\infty(\phi)] < \infty$ for $b \equiv 2, 3 \pmod{5}$ and $b \equiv 1, 2, 5, 6 \pmod{7}$. In addition $[C(\phi) : G_\infty(\phi)] < \infty$ for all $b \in \mathbb{Z}$ with $1 \leq |b| \leq 10,000$.*

The proofs of these two results follow lines similar to the proof of Theorem 2.4 (see Theorem 5.3 of [25] and the remark following for an analogue of Theorem 2.4). On the one hand, the argument requires developing considerable machinery to handle the fact that ϕ is a rational function rather than a polynomial, but on the other hand it is easier in that 0 has an extremely simple orbit under ϕ , being sent directly to the fixed point ∞ . Another key to the proof is that there is essentially only one critical orbit whose arithmetic one must keep track of: while technically there are two, one is the image of the other under $x \mapsto -x$. As with the maps in Theorem 2.4, one finds that $[C(\phi) : G_\infty(\phi)] < \infty$ follows from the seemingly much weaker assertion that the numerators of $\phi^n(x)$ are irreducible for all $n \geq 1$.

In light of the analysis in [25], we make the following conjecture:

Conjecture 3.9 ([25]). *Let $K = \mathbb{Q}$. If $\phi(x) = \frac{b(x^2+1)}{x}$ with $b \in \mathbb{Q}$ and $b \notin \{0, \pm \frac{1}{2}\}$, then $[C(\phi) : G_\infty(\phi)] < \infty$.*

Our restriction to the family in (18) is not as significant as it may seem, as every degree 2 rational function that commutes with a non-trivial Möbius function is conjugate to one of the form (18) (see [25, Section 2]). Indeed, Conjecture 3.9 is equivalent to the $K = \mathbb{Q}$ case of the following conjecture:

Conjecture 3.10 ([25]). *Let K be a global field of characteristic 0 or > 2 , and suppose $\phi(x) \in K(x)$ has degree 2. Assume that ϕ is not post-critically finite and 0 is not periodic under ϕ . If ϕ commutes with a non-trivial Möbius transformation that fixes 0, then $[C(\phi) : G_\infty(\phi)] < \infty$.*

3.5. A conjecture for quadratic rational functions. In light of the results on quadratic rational functions given in the previous four subsections we pose the following conjecture:

Conjecture 3.11. *Let K be a global field and suppose that $\phi \in K(x)$ has degree two. Then $[\text{Aut}(T_\infty) : G_\infty(\phi)] = \infty$ if and only if one of the following holds:*

- (1) *The map ϕ is post-critically finite.*
- (2) *The two critical points γ_1 and γ_2 of ϕ have a relation of the form $\phi^{r+1}(\gamma_1) = \phi^{r+1}(\gamma_2)$ for some $r \geq 1$.*
- (3) *The root 0 of T_∞ is periodic under ϕ .*
- (4) *There is a non-trivial Möbius transformation that commutes with ϕ and fixes 0.*

Our rationale for this conjecture is as follows. Thanks to the result of [40] given in (13), any quadratic rational map not satisfying condition (1) or (2) of the conjecture must satisfy $G^{\text{arith}} = \text{Aut}(T_\infty(t))$. Hence these are the only quadratic maps for which there may be a geometric reason that $[\text{Aut}(T_\infty) : G_\infty(\phi)] = \infty$. Among quadratic maps with $G^{\text{arith}} = \text{Aut}(T_\infty(t))$, the only known examples where $[\text{Aut}(T_\infty) : G_\infty(\phi)] = \infty$ are those satisfying conditions (3) and (4). The meat of the conjecture is that these are all such examples.

We remark that if ϕ satisfies one of the four conditions of Conjecture 3.11, then indeed $[\text{Aut}(T_\infty) : G_\infty(\phi)] = \infty$. This is thanks to Theorem 3.1, results of R. Pink [40, Theorem 4.8.1(b) and Corollary 4.8.9], and the fact that $[\text{Aut}(T_\infty) : \text{Stab}_\infty] = [\text{Aut}(T_\infty) : C(\phi)] = \infty$, where Stab_∞ is defined in Section 3.2 and $C(\phi)$ is the centralizer in $\text{Aut}(T_\infty)$ of the action of $x \mapsto -x$ on T_∞ . The “only if” part of Conjecture 3.11 remains wide open.

4. DENSITY RESULTS

Let us return now to the study of the density of prime divisors of orbits of rational functions, which motivated the initial investigations into arboreal representations. We show in this section that, happily, one may obtain zero-density results with a significantly weaker hypothesis than $G_\infty(\phi)$ having finite index in a known subgroup of $\text{Aut}(T_\infty)$.

For a general global field K , we have two notions of density available for a set S of primes of K :

$$\lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{q} \in S} N(\mathfrak{q})^{-s}}{\sum_{\mathfrak{q}} N(\mathfrak{q})^{-s}} \quad \text{and} \quad \limsup_{x \rightarrow \infty} \frac{\#\{\mathfrak{q} \in S : N(\mathfrak{q}) \leq x\}}{\#\{\mathfrak{q} : N(\mathfrak{q}) \leq x\}},$$

where $N(\mathfrak{q}) = \#(\mathcal{O}_K/\mathfrak{q}\mathcal{O}_K)$, and the sum in each denominator runs over all primes of K . The quantity on the left is called *Dirichlet density*, while that on the right is *natural density*. When the natural density of S exists, then so does its Dirichlet density, and the two coincide. Moreover, there are sets for which the Dirichlet density exists but the natural density does not. Natural density earns its name because it corresponds more closely to the intuitive notion of the limiting probability as $x \rightarrow \infty$ that a randomly chosen prime $\leq x$ belongs to S . Because of the differences in the versions of the Chebotarev density theorem that hold over function fields and number fields (see [43, p.125] for the former and [31, p. 368] for the latter), we use Dirichlet density in the function field setting and natural density in the number field setting. From now on, this is what we mean by “the density” of a set of primes.

Let K be a global field, $\phi \in K(x)$, and $a_0 \in K$. Let $v_{\mathfrak{p}}$ denote the \mathfrak{p} -adic valuation for a prime \mathfrak{p} of K , and define

$$P_{\phi}(a_0) := \{\mathfrak{p} : v_{\mathfrak{p}}(\phi^i(a_0)) > 0 \text{ for at least one } i \geq 0 \text{ with } \phi^i(a_0) \neq 0\}.$$

We denote $v_{\mathfrak{p}}(\phi^i(a_0)) > 0$ by $\mathfrak{p} \mid \phi^i(a_0)$. As noted in the discussion on p. 2, when $\phi(x)$ is a polynomial, the density of the complement of $P_{\phi}(a_0)$ is bounded below by the density of \mathfrak{p} such that $\phi^n(x) \equiv 0 \pmod{\mathfrak{p}}$ has no solution. For if \mathfrak{p} satisfies this condition, then we cannot have $\mathfrak{p} \mid \phi^j(a_0)$ for $j \geq n$, since otherwise $\phi^n(x) \equiv 0 \pmod{\mathfrak{p}}$ has a solution with $x = \phi^{j-n}(a_0)$. However, only finitely many \mathfrak{p} satisfy $\mathfrak{p} \mid \phi^j(a_0)$ for $0 \leq j < n$. A similar conclusion holds when ϕ is a rational function, but one must require $\phi^n(\infty) \neq 0$ and discard the finitely many \mathfrak{p} dividing $\phi^n(\infty)$ and where ϕ has bad reduction. See [25, Theorem 6.1] for details.

Now $\phi^n(x) \equiv 0 \pmod{\mathfrak{p}}$ having no solution is equivalent to Frobenius at \mathfrak{p} acting without fixed points on the elements of $\phi^{-n}(0)$. One then gets from the Chebotarev density theorem that the density of $P_{\phi}(a_0)$ is bounded above by the proportion of elements of $G_n(\phi)$ that act on $\phi^{-n}(0)$ with at least one fixed point. This holds for any n , and it follows that $P_{\phi}(a_0)$ has density zero provided that

$$(19) \quad \lim_{n \rightarrow \infty} \frac{\#\{g \in G_n(\phi) : g \text{ fixes at least one element of } \phi^{-n}(0)\}}{\#G_n(\phi)} = 0.$$

The sequence in the limit is non-increasing, for if $g \in G_n(\phi)$ acts on $\phi^{-n}(0)$ without fixed points, then the same is true of all $g' \in G_{n+1}(\phi)$ that restrict to g . Therefore the limit in (19) exists.

In the relatively rare cases where $G_n(\phi)$ is known explicitly for all $n \geq 1$, the limit in (19) can be calculated directly. The following result combines [25, Theorem 6.2] and [21, Propositions 5.5, 5.6].

Theorem 4.1. *Let K be a global field, let $\phi(x) \in K(x)$, and let $C(\phi)$ be defined as in the discussion following (18). If $G_{\infty}(\phi) = \text{Aut}(T_{\infty})$ or $G_{\infty}(\phi) = C(\phi)$, then the density of $P_{\phi}(a_0)$ is zero for all $a_0 \in K$.*

This establishes zero-density results for orbits of the ϕ given in Theorems 2.3 and 3.7, as well as the map in (6). A better result will supersede this, however, once we introduce some new ideas that allow for a similar conclusion with vastly less knowledge of $G_\infty(\phi)$. In early 2004, the author was able to establish an important fact about $G_\infty(\phi)$ (see (22)) in the setting $K = \mathbb{F}_p(t)$ (p an odd prime) and $\phi(x) = x^2 + t$, but saw no way to translate this into a form that would help prove (19). However, in a fortuitous conversation after a basketball game, A. Hoffman (then an applied math graduate student at Brown University) suggested that a convergence theorem from probability theory might be just the ticket. The resulting change in viewpoint led to the main theorems of [21], and, not coincidentally, the author's successful completion of graduate school.

In light of (19), we wish to measure the probability of a randomly chosen element of $G_n(\phi)$ belonging to the set given in the numerator of the expression in (19), and more precisely how this probability evolves as n grows. It's useful therefore to associate to a given $g \in G_n(\phi)$ the sequence $X_1(g), X_2(g), \dots, X_n(g)$, where $X_i(g)$ is the number of elements of $\phi^{-i}(0)$ fixed by g (recall that g acts on $\phi^{-i}(0)$ for $1 \leq i \leq n$ through the restriction map $G_n(\phi) \rightarrow G_i(\phi)$). If the limit in (19) is zero, then when n is large almost any choice of g will result in a sequence that has reached zero by the n th term. To understand the actual limit as n tends to infinity, we should work in $G_\infty(\phi)$, and use the restriction maps $\pi_i : G_\infty(\phi) \rightarrow G_i(\phi)$. Happily, $G_\infty(\phi)$ has a natural probability measure \mathbf{P} given by the normalized Haar measure, with the excellent property that for any $S \subseteq G_i(\phi)$, $\mathbf{P}(\pi_i^{-1}(S)) = \#S/\#G_i(\phi)$. We can now translate (19) into

$$(20) \quad \lim_{n \rightarrow \infty} \mathbf{P}(g \in G_\infty(\phi) : X_n(g) > 0) = 0.$$

To each $g \in G_\infty(\phi)$, we attach the infinite sequence $X_1(g), X_2(g), \dots$. Note that the X_i are random variables on the probability space $G_\infty(\phi)$, and probabilists are wont to give any infinite sequence of random variables on a fixed probability space the fancy-sounding moniker *stochastic process*. As this process X_1, X_2, \dots encodes information about the Galois action on T_∞ , we call it the *Galois process* of ϕ .

This rephrasing of our group theory problem in probabilistic terms has value in that it allows us to use the considerable machinery of the theory of stochastic processes. Because $\lim_{n \rightarrow \infty} \mathbf{P}(S_n) = \mathbf{P}(\bigcap S_n)$ for any nested sequence of sets S_n , (20) is equivalent to the statement that almost all sequences $X_1(g), X_2(g), \dots$ are eventually zero. To prove this, we use two steps:

- (A) Show that almost all sequences $X_1(g), X_2(g), \dots$ are eventually constant.
- (B) Show that if $r > 0$, then for infinitely many $n \geq 1$ we have

$$\mathbf{P}(X_n(g) = r \mid X_{n-1}(g) = r) \leq 1 - \epsilon,$$

where $\epsilon > 0$ is independent of n .

Condition (B) ensures that the probability of $X_1(g), X_2(g), \dots$ being eventually constant at a fixed $r > 0$ is zero, and the desired conclusion follows. While step (A) may

not seem the most obvious way to proceed, it fits nicely with the notion of convergence of a stochastic process: the process X_1, X_2, \dots converges if there exists a random variable $X : G_\infty \rightarrow \mathbb{R}$ such that $X_n \rightarrow X$ almost surely, or in other words,

$$\mathbf{P}(g \in G_\infty(\phi) : \lim_{n \rightarrow \infty} X_n(g) \text{ exists}) = 1.$$

Because the X_n are integer-valued, this implies that the sequence $X_1(g), X_2(g), \dots$ is eventually constant with probability one, just as in (A) above.

But how to show the Galois process converges? It is here that we call on substantial ideas from probability theory, which has a plethora of results giving sufficient conditions for a stochastic process to converge. One kind of process for which powerful convergence theorems exist is called a *martingale*, which roughly is a “locally fair” process in that the expected behavior one step into the future, given a certain present behavior, is always the same as the present behavior. More precisely, for all $n \geq 2$ and any $t_i \in \mathbb{R}$,

$$(21) \quad E(X_n \mid X_1 = t_1, X_2 = t_2, \dots, X_{n-1} = t_{n-1}) = t_{n-1},$$

provided $\mathbf{P}(X_1 = t_1, X_2 = t_2, \dots, X_{n-1} = t_{n-1}) > 0$. Martingales often converge; in particular [13, Section 12.3] gives the highly useful result that if the random variables of a martingale take non-negative values, then the martingale converges. Certainly in the present case $X_n(g) \geq 0$ for all $g \in G_\infty(\phi)$. To sum up, then, we may accomplish step (A) above simply by showing that the Galois process is a martingale.

To establish (21) for the Galois process involves examining all lifts to $G_n(\phi)$ of a given $g_0 \in G_{n-1}(\phi)$. Indeed, conditioning on the behavior $X_1 = t_1, X_2 = t_2, \dots, X_{n-1} = t_{n-1}$ is the same as restricting consideration to a certain subset S of $G_{n-1}(\phi)$, and then looking at the expected value of $X_n(g)$ as $g \in G_n(\phi)$ varies over elements restricting to S . If we can show that the expected value of $X_n(g)$ is t_{n-1} for lifts of each $g_0 \in S$ individually, then (21) immediately follows.

Now the set of all lifts to $G_n(\phi)$ of $g_0 \in G_{n-1}(\phi)$ is just the coset gH_n , where g is any lift of g_0 and

$$H_n = \{h \in G_n(\phi) : h \text{ restricts to the identity on } G_{n-1}(\phi)\}.$$

If we let $K_n = K(\phi^{-n}(0))$, then H_n is the Galois group of the relative extension K_n/K_{n-1} . Because we are conditioning on $X_1 = t_1, X_2 = t_2, \dots, X_{n-1} = t_{n-1}$, we may assume that g_0 has t_{n-1} fixed points in $\phi^{-(n-1)}(0)$. Let α be one such fixed point, and note that to establish (21) it is enough to show that on average an element of gH_n fixes one point in $\phi^{-1}(\alpha)$, for then the average total number of fixed points of an element of gH_n acting on $\phi^{-n}(0)$ is t_{n-1} . Now if

$$(22) \quad H_n \text{ acts transitively on every set of the form } \phi^{-1}(\alpha),$$

then an application of Burnside’s lemma gives the desired result. In the case where ϕ is a polynomial, (22) is equivalent to $\phi(x) - \alpha$ being irreducible over K_{n-1} for each root α of $\phi^{n-1}(x)$. See [22, Theorem 2.5] for a slightly more general version of this statement.

Establishing (22) is difficult in general, but turns out to be tractable in many circumstances. In the geometric setting considered in [19], it is an easy result (see the remarks following Theorem 5.1 of [19]). The first result in an arithmetic setting appeared in [21, Theorem 1.2], in the case where ϕ is a quadratic polynomial over a field of characteristic $\neq 2$ satisfying a hypothesis that essentially says the critical orbit of ϕ contains no squares. A mild generalization, allowing roughly for a finite number of squares to occur in the critical orbit of ϕ , appeared in [22, Theorem 2.7]. In particular this result implies that if ϕ is quadratic with all iterates irreducible, then (22) holds for sufficiently large n , and this is enough to establish (A). A more significant generalization to certain polynomials of the form $x^p + b$, where p is prime, has recently been given in [14, Theorem 3.4], under the hypothesis that the ground field K contains a primitive p th root of unity. The proofs of all these theorems rely on a careful study of permutation groups with certain properties. A different approach is taken in [14, Theorem 3.3], where a much more straightforward local argument suffices to prove (22) for $\phi(x) = x^d + b$ under the slightly more restrictive hypothesis that $v_{\mathfrak{p}}(b) > 0$ for some prime \mathfrak{p} of K of residue characteristic not dividing d , but with the great added advantage of holding for composite d . Again, K is assumed to contain a primitive d th root of unity.

We turn now to proving (B), the second step in the two-step program given on p. 22. As in step (A), the probability involved is conditioned on the value of $X_{n-1}(g)$, and thus we may restrict consideration to cosets of H_n . The key advantage is that *we only need knowledge of H_n for infinitely many n* . In many cases it is possible to precisely determine H_n for an infinite set of n . This is certainly true when $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is finite, and while the literature appears to contain no precise proof of (B) in this case, one can be adapted from [14, Lemma 4.6] (see also [35, Lemma 4.3]). This gives

Theorem 4.2. *Let K be a global field and $\phi \in K(x)$. Suppose that the Galois process for ϕ is a martingale and $[\text{Aut}(T_\infty) : G_\infty(\phi)]$ is finite. Then the density of $P_\phi(a_0)$ is zero for all $a_0 \in K$.*

In many cases, zero-density results are possible under far weaker assumptions than $[\text{Aut}(T_\infty) : G_\infty(\phi)] < \infty$. For instance, when ϕ is a quadratic polynomial, one can show under mild hypotheses that Siegel's theorem on integral points implies $H_n \cong (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}$ (that is, H_n is as large as possible) for infinitely many n . See [21, Corollary 6.6] and [22, Proof of Theorem 1.1]. In particular, one may obtain a zero-density result for primes dividing orbits of $\phi(x) = x^2 + 3$, though as mentioned on p. 6 it is not known whether $[\text{Aut}(T_\infty) : G_\infty(\phi)] < \infty$. Another interesting example is that of $\phi(x) = x^2 + t$, with $K = \mathbb{F}_p(t)$ for an odd prime p ; this is the motivating example of [21]. In this case, one can show that $H_n \cong (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}$ when n is squarefree [21, Corollary 6.6], although it remains unknown whether $[\text{Aut}(T_\infty) : G_\infty(\phi)] < \infty$ (see Conjecture 6.7 of [21]). This yields a zero-density result for prime divisors of orbits of ϕ , and in particular for prime

divisors of the sequence

$$\{t, t^2 + t, t^4 + 2t^3 + t^2 + t, \dots\},$$

which is the orbit of 0 under ϕ in $\mathbb{F}_p[t]$. This has consequences for the p -adic Mandelbrot set, in particular showing that its hyperbolic subset is small in a certain sense (see Theorem 1.4 of [21]). A further interesting family of examples is given by $\phi(x) = x^d + b$. For this family, it's shown in [14, Theorem 4.5] that $H_n \cong (\mathbb{Z}/d\mathbb{Z})^{d^{n-1}}$ for infinitely many n , under mild conditions on b . This leads to corresponding zero-density results (see Theorem 1.1 of [14], or part (5) of Theorem 4.3 below). A crucial caveat in all the results mentioned in this paragraph is that they require that all iterates of ϕ be irreducible, pointing up once again the importance of this property.

As a final note, many of the polynomial results cited in this section are proven for *translated iterates*, that is, polynomials of the form $g \circ \phi^n(x)$, where $g(x)$ divides some iterate of ϕ . This presents only mild complications and allows one to obtain density results in the situation where some iterates of $\phi(x)$ are reducible, provided that the number of irreducible factors of $\phi^n(x)$ is bounded as n grows (in the terminology of Section 5, ϕ is *eventually stable*). For example, this makes possible density results about $\phi(x) = x^2 - 4$, which has the property that for each $n \geq 1$, $\phi^n(x)$ is the product of two irreducible polynomials over \mathbb{Q} (see [22, Section 4]).

We now give a theorem that exemplifies the kind of result made possible by the preceding analysis. Each statement below is a special case of the theorem cited.

Theorem 4.3. *For the following $\phi \in \mathbb{Q}(x)$, $P_\phi(a_0)$ has density zero for all $a_0 \in \mathbb{Q}$:*

- (1) $\phi(x) = x^2 + kx - k$ for $k \in \mathbb{Z}$ [22, Theorem 1.2]
- (2) $\phi(x) = x^2 + kx - 1$ for $k \in \mathbb{Z} \setminus \{0, 2\}$ [22, Theorem 1.2]
- (3) $\phi(x) = x^2 + k$ for $k \in \mathbb{Z} \setminus \{-1\}$ [22, Theorem 1.2]
- (4) $\phi(x) = \frac{k(x^2+1)}{x}$ for odd $k \in \mathbb{Z}$ having no prime factor $\equiv 1 \pmod{4}$ [25, Corollary 5.14, Theorem 6.2]

Moreover, if p is an odd prime, K is a number field containing a primitive p th root of unity, and

- (5) $\phi(x) = x^p + k$ for $k \in \mathbb{Z}$,

then $P_\phi(a_0)$ has density zero for all $a_0 \in K$ [14, Corollary 1.3].

5. STABILITY AND EVENTUAL STABILITY

As noted frequently in Sections 2 and 4, establishing the transitivity of the action of $G_n(\phi)$ on the sets $\phi^{-n}(0)$ is crucial to understanding $G_\infty(\phi)$. Even when this transitivity fails, one can often recover significant information about $G_\infty(\phi)$ when its action on $\phi^{-n}(0)$ has a bounded number of orbits as n grows. Thus we are interested in the factorization into irreducibles of the numerator of $\phi^n(x)$. We make these definitions, where F denotes *any field*:

- $\phi \in F(x)$ is *stable* if the numerator of $\phi^n(x)$ is irreducible for all $n \geq 1$.
- $\phi \in F(x)$ is *eventually stable* if the number of irreducible factors of the numerator of $\phi^n(x)$ is bounded as n grows.

The extent to which these two properties hold for generic ϕ is a question of great interest, and which has prompted much recent research. As in the study of the Galois theory of iterates, it was Odoni who first examined questions of stability: see [35, Sections 1 and 2], [36, Proposition 4.1], and [37, Lemma 4.2]. A fundamental observation is that Eisenstein polynomials are stable, as any iterate of an Eisenstein polynomial is again Eisenstein. This statement holds in great generality, and in [35, Lemma 2.2] Odoni uses it to prove that the generic degree- d monic polynomial given in (5) is stable. When ϕ is a quadratic polynomial, recent work gives additional sufficient conditions for stability to hold. The critical point of ϕ again proves critical, just as in the questions of the maximality of H_n dealt with in Sections 2 and 4. Here are two such results:

Theorem 5.1. [23, Theorem 2.2] *Let F be any field of characteristic $\neq 2$, and let $\phi \in F[x]$ be monic and quadratic, with critical point c . Then $\phi(x)$ is stable if none of $-\phi(c), \phi^2(c), \phi^3(c), \phi^4(c) \dots$ is a square in F .*

Theorem 5.2. [23, Theorem 3.1] *Let $\phi(x) = (x - \gamma)^2 + \gamma + m$ with $\gamma, m \in \mathbb{Z}$. If $\gamma \not\equiv m \pmod{2}$, then ϕ is stable.*

Both of these results apply to many non-Eisenstein polynomials. When the field F in Theorem 5.1 is a finite field, “if” may be replaced by “if and only if,” and this stronger result underlies much of the analysis in [3]. The proof of Theorem 5.1 is a nice exercise in field theory, with the key step being to define a certain sequence $(\tau_n)_{n \geq 1}$ with $\tau_n \in F(\phi^{-n}(0))$, and to show that τ_n is not a square in $F(\phi^{-n}(0))$, for each $n \geq 1$. To do this, one takes the norm from $F(\phi^{-n}(0))$ to F of τ_n , and the result is a square times $\phi^n(c)$. Hence if $\phi^n(c)$ is not a square in F for each $n \geq 1$, the desired result follows (with an additional complication in the case $n = 1$). Theorem 5.2 is proven by taking the norm of τ_n from $F(\phi^{-n}(0))$ to $F(\phi^{-1}(0))$ instead. The version stated here is a special case of [23, Theorem 3.1], as the latter holds over most number fields.

When ϕ is a rational function, even of degree 2, there are very few results giving sufficient conditions for ϕ to be stable. One such result is for the family in (18), where a condition similar to that of Theorem 5.1 is given in [25, Theorem 4.5].

The fact that Eisenstein polynomials are stable, along with Theorems 5.1 and 5.2, suggests that stability should hold for a large class of polynomials over a given global field. Indeed, when $\phi \in \mathbb{Z}[x]$ is monic and quadratic this is a theorem (see [1], where a proof is given using Theorem 5.1). However, the notion of stability has the disadvantage of not being invariant under finite extensions of the ground field. Moreover, even for quadratic polynomials over \mathbb{Q} one finds examples where stability fails for no obvious structural reason. For instance, recall from p. 7 the case $\phi(x) = x^2 - x - 1$, where $\phi(x)$ and $\phi^2(x)$ are irreducible but $\phi^3(x)$ factors as the product of two irreducible quartics. Another interesting example is $\phi(x) = x^2 - \frac{16}{9}$, where one has not only the obvious

factorization of ϕ , but an additional splitting of ϕ^3 :

$$\phi^3(x) = \left(x^2 - 2x + \frac{2}{9}\right) \left(x^2 + 2x + \frac{2}{9}\right) \left(x^2 - \frac{22}{9}\right) \left(x^2 - \frac{10}{9}\right).$$

It is possible to prove for this example that no additional splitting occurs: for $n \geq 3$, $\phi^n(x)$ has precisely four irreducible factors over \mathbb{Q} (see the remark following the proof of Theorem 1.6 of [14]).

Eventual stability, on the other hand, may reasonably be expected to hold for all maps for which 0 is not periodic under ϕ (see the discussion at the end of Section 3.3 for the reasons why the latter must be excluded). In the case where $\phi \in \mathbb{Z}[x]$ is monic and quadratic, this is Conjecture 1 at the end of Section 4 of [22]. A more general conjecture is proposed in [24]. However, few results in this direction are known. To the author's knowledge, the most general are these:

Theorem 5.3. [14, Theorem 1.6] *Let $d \geq 2$, let K be a field of characteristic not dividing d , and let $\phi(x) = x^d + c \in K[x]$ with $c \neq 0$. If there is a discrete non-archimedean absolute value on K with $|c| < 1$, then ϕ is eventually stable over K .*

Theorem 5.4. [17, Corollary 3] *Let K be a number field and $\phi(x)$ a monic polynomial of degree d defined over K . Suppose that there exists a non-archimedean prime \mathfrak{p} of K with $\mathfrak{p} \nmid d$ and such that $|\phi^n(0)|_{\mathfrak{p}} \rightarrow \infty$ as $n \rightarrow \infty$. Then ϕ is eventually stable over K .*

See also [22, Proposition 4.5], where eventual stability is proven for some specific families of quadratic polynomials over \mathbb{Z} . Theorem 5.3 gives an especially strong result in the case where K is a global function field (or indeed a function field over any field) of characteristic not dividing d : ϕ is eventually stable unless c belongs to the field of constants of K . See [14, Corollary 1.8]. Interestingly, the maps in Theorem 5.3 satisfy $|\phi^n(0)| \rightarrow 0$ as $n \rightarrow \infty$, and so Theorems 5.3 and 5.4 apply to quite different maps. The methods of proof of both are local in nature, but the proof of Theorem 5.3 relies on the fact that factorizations of iterates of $x^d + c$ take a special form [14, Theorem 2.2], while to prove Theorem 5.4, Ingram constructs a non-archimedean version of the Böttcher coordinate [17, Theorem 2].

Questions of stability and eventual stability remain at the heart of this area, and a subject of active research. See for instance [1, 4, 7, 11, 38, 48] for further reading.

ACKNOWLEDGEMENTS

I am grateful to Richard Pink, Joe Silverman, Rob Benedetto, Ben Hutz, and Wade Hindes for valuable comments on earlier drafts of this article.

REFERENCES

- [1] Omran Ahmadi, Florian Luca, Alina Ostafe, and Igor E. Shparlinski. On stable quadratic polynomials. *Glasg. Math. J.*, 54(2):359–369, 2012.

- [2] Wayne Aitken, Farshid Hajir, and Christian Maire. Finitely ramified iterated extensions. *Int. Math. Res. Not.*, (14):855–880, 2005.
- [3] Nigel Boston and Rafe Jones. Settled polynomials over finite fields. *Proc. Amer. Math. Soc.*, 140(6):1849–1863, 2012.
- [4] Katharine Chamberlin, Emma Colbert, Sharon Frechette, Patrick Heffernan, Rafe Jones, and Sarah Orchard. Newly reducible iterates in families of quadratic polynomials. *Involve*, 5(4):481–495, 2012.
- [5] John E. Cremona. On the Galois groups of the iterates of $x^2 + 1$. *Mathematika*, 36(2):259–261 (1990), 1989.
- [6] John Cullinan and Farshid Hajir. Ramification in iterated towers for rational functions. *Manuscripta Math.*, 137(3-4):273–286, 2012.
- [7] Lynda Danielson and Burton Fein. On the irreducibility of the iterates of $x^n - b$. *Proc. Amer. Math. Soc.*, 130(6):1589–1596 (electronic), 2002.
- [8] Pierre de la Harpe. *Topics in geometric group theory*. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 2000.
- [9] Robert L. Devaney. *An introduction to chaotic dynamical systems*. Addison-Wesley Studies in Nonlinearity. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, second edition, 1989.
- [10] Xander Faber and Andrew Granville. Prime factors of dynamical sequences. *J. Reine Angew. Math.*, 661:189–214, 2011.
- [11] Domingo Gomez-Perez, Alina Ostafe, and Igor E. Shparlinski. On irreducible divisors of iterated polynomials. To appear, *Rev. Mat. Iberoam.*
- [12] Chad Gratton, Khoa Nguyen, and Thomas J. Tucker. ABC implies primitive prime divisors in arithmetic dynamic. To appear, *Bull. Lond. Math. Soc.* Available at <http://arxiv.org/abs/1208.2989>.
- [13] Geoffrey Grimmett and David Stirzaker. *Probability and random processes*. Oxford University Press, New York, third edition, 2001.
- [14] Specer Hamblen, Rafe Jones, and Kalyani Madhu. The density of primes in orbits of $z^d + c$. *Int. Math. Res. Not.* 2014; doi: 10.1093/imrn/rnt349. Available at <http://arxiv.org/abs/1303.6513>.
- [15] Wade Hindes. Arithmetic properties of curves related to dynamical Galois theory. Available at <http://arxiv.org/abs/1305.0222>.
- [16] Wade Hindes. Points on elliptic curves parametrizing dynamical Galois groups. *Acta Arith.*, 159:149–167, 2013.
- [17] Patrick Ingram. Arboreal Galois representations and uniformization of polynomial dynamics. *Bull. Lond. Math. Soc.*, 45(2):301–308, 2013.
- [18] Patrick Ingram and Joseph H. Silverman. Primitive divisors in arithmetic dynamics. *Math. Proc. Cambridge Philos. Soc.*, 146(2):289–302, 2009.
- [19] Rafe Jones. Fixed-point-free elements of iterated monodromy groups. To appear, *Trans. Amer. Math. Soc.* Available at <http://arxiv.org/abs/1204.2843>.
- [20] Rafe Jones. *Galois martingales and the hyperbolic subset of the p -adic Mandelbrot set*. PhD thesis, Brown University, 2005.
- [21] Rafe Jones. Iterated Galois towers, their associated martingales, and the p -adic Mandelbrot set. *Compos. Math.*, 143(5):1108–1126, 2007.
- [22] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)*, 78(2):523–544, 2008.
- [23] Rafe Jones. An iterative construction of irreducible polynomials reducible modulo every prime. *J. Algebra*, 369:114–128, 2012.
- [24] Rafe Jones and Alon Levy. Eventually stable rational functions. In preparation.

- [25] Rafe Jones and Michelle Manes. Galois theory of quadratic rational functions. To appear, *Comment. Math. Helv.* Available at <http://arxiv.org/abs/1101.4339>.
- [26] Holly Krieger. Primitive prime divisors in the critical orbit of $z^d + c$. *Int. Math. Res. Not.* 2012; doi: 10.1093/imrn/rns213. Available at <http://arxiv.org/abs/1203.2555v2>.
- [27] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [28] Michelle Manes and Diane Yap. A census of quadratic post-critically finite rational maps defined over \mathbb{Q} . Available at <http://arxiv.org/abs/1212.1518>.
- [29] Patrick Morton. Galois groups of periodic points. *J. Algebra*, 201(2):401–428, 1998.
- [30] Patrick Morton and Pratiksha Patel. The Galois theory of periodic points of polynomial maps. *Proc. London Math. Soc. (3)*, 68(2):225–263, 1994.
- [31] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.
- [32] Volodymyr Nekrashevych. *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.
- [33] Volodymyr Nekrashevych. Iterated monodromy groups. In *Groups St Andrews 2009 in Bath. Volume 1*, volume 387 of *London Math. Soc. Lecture Note Ser.*, pages 41–93. Cambridge Univ. Press, Cambridge, 2011.
- [34] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.
- [35] R. W. K. Odoni. The Galois theory of iterates and composites of polynomials. *Proc. London Math. Soc. (3)*, 51(3):385–414, 1985.
- [36] R. W. K. Odoni. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. *J. London Math. Soc. (2)*, 32(1):1–11, 1985.
- [37] R. W. K. Odoni. Realising wreath products of cyclic groups as Galois groups. *Mathematika*, 35(1):101–113, 1988.
- [38] Alina Ostafe and Igor E. Shparlinski. On the length of critical orbits of stable quadratic polynomials. *Proc. Amer. Math. Soc.*, 138(8):2653–2656, 2010.
- [39] Richard Pink. Finiteness and liftability of postcritically finite quadratic morphisms in arbitrary characteristic. Available at <http://arxiv.org/abs/1305.2841>.
- [40] Richard Pink. Profinite iterated monodromy groups arising from quadratic morphisms with infinite postcritical orbits. Available at <http://arxiv.org/abs/1309.5804>.
- [41] Richard Pink. Profinite iterated monodromy groups arising from quadratic polynomials. Available at <http://arxiv.org/abs/1307.5678>.
- [42] Brian Rice. Primitive prime divisors in polynomial arithmetic dynamics. *Integers*, 7:A26, 16, 2007.
- [43] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [44] Jean-Pierre Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
- [45] Joseph H. Silverman. Primitive divisors, dynamical Zsigmondy sets, and Vojta’s conjecture. Available at <http://arxiv.org/abs/1209.3491>.
- [46] Joseph H. Silverman. The field of definition for dynamical systems on \mathbf{P}^1 . *Compositio Math.*, 98(3):269–304, 1995.
- [47] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
- [48] Vijay A. Sookdeo. Integer points in backward orbits. *J. Number Theory*, 131(7):1229–1239, 2011.

- [49] Peter Stevenhagen and Hendrik W. Lenstra, Jr. Chebotarëv and his density theorem. *Math. Intelligencer*, 18(2):26–37, 1996.
- [50] Michael Stoll. Galois groups over \mathbf{Q} of some iterated polynomials. *Arch. Math. (Basel)*, 59(3):239–244, 1992.